

Sample Checklists for Conducting Internal Monitoring and Auditing

A well-designed compliance program should include both external and internal auditing.[1] Independent auditors, program integrity contractors, or regulatory agencies conduct external audits, while providers conduct their own internal audits. This job aid will help providers conduct internal monitoring and auditing of electronic health records (EHRs). It may also help managed care plans and other ancillary entities that may conduct or assist in monitoring or auditing EHRs. The initial discussion in this job aid addresses using automated vendor or third-party software to monitor for potential fraud, waste, and abuse in EHRs. Further discussion addresses periodic internal auditing and auditing providers should conduct to follow up on items identified through monitoring as possible instances of fraud, waste, or abuse. For information on internal monitoring and auditing for program integrity issues in general, refer to the “Conducting a Self-Audit: A Guide for Physicians and Other Health Care Professionals” booklet, which is part of the Audit Toolkit posted to <https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/audit-toolkit.html> on the Centers for Medicare & Medicaid Services (CMS) website.

Internal Monitoring

Monitoring is an ongoing effort “to ensure that policies and procedures are in place and are being followed.”[2] It takes place on a regular basis during normal operations.[3] There are several reasons for providers to implement an internal monitoring program to detect unauthorized access to or use of patient EHRs. These reasons include:

- As “covered entities” under the Health Insurance Portability and Accountability Act’s (HIPAA)[4] Privacy Rule,[5] providers are required to take appropriate steps to protect EHRs from unauthorized access.[6] Failure to take these steps can lead to civil monetary penalties;[7]
- CMS requires certain managed care plans to conduct internal monitoring and auditing for potential fraud, waste, and abuse as one of the seven elements of an effective compliance program;[8] and



- The U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG) recommends conducting internal monitoring and auditing.[9]

Providers who want to purchase a new EHR system or upgrade an existing system should ask vendors whether automated monitoring and reporting capabilities are available. Providers may also want to consider purchasing third-party software or services to add fraud, waste, and abuse detection capabilities to their systems. In 2005, the American Health Information Management Association predicted that customized fraud detection software would eventually become as widely available in the health care field as it is in banking and financial services.[10] An industry article from 2014 indicates this prediction is coming true. The article notes that CMS and the Massachusetts health insurance exchange use automated fraud detection software, and cites a report that 97 percent of payers surveyed planned to invest in their fraud, waste, and abuse detection systems in 2014–15.[11]

For now, fraud detection software is not standard in certified EHR systems, and HHS-OIG recently released a report[12] encouraging CMS to provide guidance to EHR users on how to detect fraud, and more specifically how to use the audit logs, which are now required by rule in certified EHR software.[13] Many providers, especially small and solo provider practices, may not be able to afford new or upgraded software or third-party monitoring services to automate their monitoring efforts. However, these providers can still lay the foundation for a basic monitoring program by controlling access to EHRs and authorizing certain tasks only to those who need to perform those tasks. For example, both billing personnel and medical professionals need access to the content of medical records, but typically, only the medical professionals would be in a position to revise or add to the content.

Providers can then establish a process to manually examine randomly selected EHRs and their corresponding audit log entries. This approach is discussed in the “Manual Review of Electronic Health Records” job aid, and the booklet, “Detecting and Responding to Fraud, Waste, and Abuse Associated With the Use of Electronic Health Records,” both posted to <https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html> on the CMS website.

Regardless of whether monitoring occurs through automated software, or through random sampling and manual inspection, providers should take similar steps to complete the process. These steps are:

1. Identify risks.
2. Do a baseline audit.
3. Develop and implement a plan for ongoing monitoring.
4. Perform corrective action.

1. Identify Risks

The first step in the monitoring process is to develop a method to identify program integrity risks. CMS recommends the compliance officer or designee work with the organization's multidisciplinary compliance committee to identify the operational risk areas and related vulnerabilities.[14] The compliance committee should include senior representatives from relevant operational areas,[15] including finance, internal audit, human resources, licensing and credentialing, contract management, legal, and investigations. For small practices, the compliance designee should consult persons with responsibility for billing and for the EHR system. Common areas to review for program integrity risks may include:

- Compliance with Federal and State privacy and security regulations and guidance, or internal policy; and
- Risk areas that may have been identified through:
 - Risk analysis;
 - Fraud detection software; or
 - Experience (for example, a high number of rejected claims or high instance of password sharing).

Common EHR program integrity risks include:

- Unauthorized access to EHRs;
- Overdocumentation, or misuse of auto-fill features (macros, templates);
- Upcoding;
- Misuse of copy and paste;
- Misuse of copy forward;
- Disabling audit logs; and
- Disabling system warnings and alerts.

Once an organization identifies the program integrity risks, they should complete an initial assessment to establish a baseline measure.[16]

2. Do a Baseline Audit

HHS-OIG recommends that before establishing the internal monitoring and auditing elements of a compliance program, providers do a baseline audit, or snapshot, of the claims development and submission process over a period of 3 months. They can use the results of that audit to identify the areas that should be the subject of ongoing

monitoring and periodic audits.[17] Doing a baseline audit for EHR compliance with security, coding, billing, and documentation requirements, whether as part of an overall compliance audit or as a separate effort, should serve the same purpose. The compliance officer or designee and monitoring team should work with the system administrator to identify the queries or methods to put into place to identify noncompliance through a baseline audit. Vendor or third-party software may also offer system edits or have built-in algorithms to identify potential fraud, waste, abuse, and improper payments.

Systems certified by the U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology (ONC), must have the capability to sort log entries and create audit reports for specific time periods.[18] This capability can be useful in developing a baseline audit, but systems that meet the minimum certification requirements may not perform this function efficiently.[19, 20] Third-party software may be necessary and can address this problem. For example, third-party software can load EHR access data from the audit log into a separate database and then analyze the data through statistical and machine-learning methods. One study has shown this to be an effective approach to identifying suspicious incidents.[21] Small providers and others for whom buying such software is not feasible can still do a simple baseline audit by manually reviewing a random sample of records and their associated claims and audit log entries. Small providers can follow a similar procedure to the one described by HHS-OIG for performance of a baseline general compliance audit by a small provider.[22]

Sample Checklist 1. Events provides some event questions, based on regulations and experience, to include as part of a baseline audit. Check the “Yes” box for each question found to be true during the baseline audit. Check the “No” box for each question found to be false during the baseline audit. If an event is marked with a “Yes” in this toolbox, take remedial action to correct it.

Sample Checklist 1. Events

Events*	Yes or No
Has the audit log function been disabled at any time?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are known changes to data entries missing from the audit log?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Is there evidence that the audit log has been altered?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Has the encryption status been disabled, either on the server or locally on end-user devices?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are unauthorized employees able to disable the audit log?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Were there changes to the EHR software program?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Events*	Yes or No
Was there duplicate text in a patient's record on different dates or for different providers that treat the patient (cloning)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Was there duplicate text from the health record of one provider's patient in the record of another provider's patient (clinical plagiarism)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Were notes entered by personnel, other than the attending or supervising provider, which the provider did not validate?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are there an unusually large number of certain types of transactions?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are there transactions that reflect unusually large dollar amounts?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are there abnormal types of transactions?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are there an unusually large number of patient information views, especially by one or a few unauthorized individuals?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Have any employees viewed records they would not ordinarily need to see?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are there unauthorized views of EHRs for friends and relatives (especially of the one accessing the records), celebrities, or minors being treated for pregnancy or other sex-related conditions?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Have any incident reports not been evaluated to determine the cause or source of the incident?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are system warning messages and responses disabled?	<input type="checkbox"/> Yes <input type="checkbox"/> No

* Find other ideas for the questions for this checklist on the Internet at:

- http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050599.hcsp?dDocName=bok1_050599
- <http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf>
- <https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf>

Incident reports describe actual or alleged events involving a patient, employee, volunteer, or visitor that puts themselves or others at risk.[23] In health care, incidents reported are usually critical incidents or adverse events that may cause or have caused patient harm or death. Larger health care entities maintain a list of suggested reportable events that include items that can involve the EHR system, such as medication errors, diagnostic or therapeutic procedure errors, lost or stolen patient records, privacy violations, and security violations.[24, 25] These errors and violations can affect quality of care and can lead to fraud, waste, or abuse. As part of the internal monitoring process, providers and others should educate staff on reportable incidents, and evaluate any reported incidents to see if the error was related to EHR use.

One suggestion for detecting cloning and clinical plagiarism in EHRs is to use the same software academic institutions employ to detect plagiarism in student work.[26] Duplication of text is not always inappropriate, but it can indicate the need for scrutiny. A study published in 2013 successfully used such software to measure the extent of copying and pasting in an intensive care unit.[27]

3. Develop and Implement a Plan for Ongoing Monitoring

The next step in the monitoring process is to develop a plan for constant monitoring. The plan should incorporate specific ongoing processes for identifying each type of noncompliance identified as problematic in the baseline. Providers can apply many of the methods used in performing the baseline audit to the ongoing monitoring plan. For example, methods used in the baseline audit to identify excessive copying and pasting can be incorporated in ongoing monitoring programs. If the audit identifies unauthorized access to EHR data as a risk, there is software that can assist in tracking and reporting access.

Methods providers and others may use for identifying unauthorized EHR access as part of ongoing monitoring may include:

- Collecting electronic data on the date and time of access events;
- Collecting electronic user access and patient data near the time of events;
- Putting data collected into a database so that it can be analyzed by a variety of programs without impeding the computer system's capacity to handle ongoing operations dealing with the same data;
- Performing data mining to identify possible unauthorized access events;
- Developing electronic reports for further investigation; and
- Evaluating reports to identify false positives and adjusting accordingly.[28]

Assessment methods may include accessing and comparing multiple systems. For example, when looking for unauthorized access to EHRs of employees or their relatives, the provider may need to query both EHR data and human resources (HR) systems.[29]

The monitoring plan should include:

- How often system reports should run;
- Time frames of the data within the reports;
- Person(s) responsible for analysis of the data; and

- Time frames for delivery of analytical reports to the compliance officer or designee.

There should be a designated person responsible for implementing and tracking the monitoring plan. It is helpful to develop a monitoring plan tracking tool to make sure to address all identified program integrity risk areas.[30]

4. Perform Corrective Action

Those responsible should analyze each monitoring report and identify changes from the baseline audit outcomes. An anomaly could indicate the EHR monitoring and reporting process is flawed and requires further review. Investigate changes in measures from the baseline audit for possible unauthorized or suspicious activity.

Once the provider identifies an issue through data analysis, they should develop and implement a plan for corrective action. This plan may include employee discipline, modification of software, changes in policy, and referral to State or Federal agencies. In general, HHS-OIG expects managed care plans to report violations of the law to HHS-OIG and CMS within 30 days.[31] Contract provisions or State Medicaid agency procedures may require reporting to other entities or reporting within different periods. After implementing corrective action, the provider should include analysis of how effective the corrective actions are in the monitoring reports.

Internal Audits

Providers should examine incidents that internal monitoring identifies as suspicious. If a short examination does not resolve the incident, and if the incident does not require immediate referral to law enforcement, an internal audit should further examine the incident.

An internal audit is different from monitoring in that it is done periodically rather than on an ongoing basis. An internal audit is more focused, more comprehensive, and based on specific predetermined standards. Internal audits to determine compliance with the predetermined standards should occur at least once a year.[32, 33] The persons who conduct the audits should be different from those who conduct monitoring.[34] Those who conduct the audits should have knowledge and experience related to the risk areas under review.[35]

HHS-OIG recommends that periodic audits focus on areas in which the provider has identified a risk of noncompliance.[36] Therefore, providers seeking to ensure compliance with EHR program integrity requirements should use periodic internal audits to determine whether the monitoring program is doing an adequate job in detecting unauthorized access and other risks to the integrity of EHRs.

In general, the steps for an internal audit of EHRs are the same as for any other internal audit, and include the following:

1. Identify the risks;
2. Audit the risks;
3. Document the audit by stating:
 - a. Where the information came from;
 - b. Why the information was gathered;
 - c. What the information means; and
 - d. What was done with the information;
4. Review and act on the audit results.

The next section reviews the steps for an internal audit in more detail.

1. Identify the Risks

Providers should periodically audit the program integrity risk areas that are part of their internal monitoring plan. In addition, providers should consider auditing other risk areas based on their experience, or the experiences of other providers. Providers and others can identify other risks by using risk assessment tools that are available commercially or free of charge from the websites of compliance organizations.[37]

2. Audit the Risks

Sample Checklist 2. Internal Audit Findings provides common items providers should check to ensure they are functioning during an internal audit. Recognizing these items is a method for discovering EHR fraud, waste, and abuse. Only answer the question “Yes” if there are no exceptions. Otherwise, answer “No.” If an item is marked “No,” plan and implement corrective action.

Sample Checklist 2. Internal Audit Findings

Audit Questions:	Yes or No
Is the audit log complete and functional?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are there adequate limitations on access to EHRs that are properly enforced?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are data in transit and in storage adequately encrypted?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are stored data adequately protected from outside intruders or hackers?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are there adequate controls requiring outside approval before any one person can make changes to the EHR system?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Audit Questions:	Yes or No
Is the EHR system in compliance with the ONC certification standards if the plan or provider receives incentive payments?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are there adequate procedures in place to preserve data in the case of catastrophic system failure?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are there adequate controls in place to ensure the integrity of records? For example: Is text from multiple authors attributed correctly? Are amendments distinguishable from the original text? and Are amendments correctly dated and attributed?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are diagnoses supported by observations, examinations, and tests, and do they support claims?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does identical text appearing within a patient record or in two different patients' records accurately reflect each patient's history, condition, and treatment?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are suspicious patterns of access to EHRs identified by monitoring justified by established policies and procedures?	<input type="checkbox"/> Yes <input type="checkbox"/> No

3. Document the Audit

Audit reports should document periodic audits. The reports should provide “reasonable assurance that evidence is sufficient and appropriate to support the auditors’ findings and conclusions.”[38] The goal is to make it clear to a third party that the findings in the report are reasonable and that the auditor used a reasonable process to reach them. A useful approach is to state where the information came from, why the information was gathered, what the auditor did with the information, what the auditor learned from the information, and what conclusions to draw. Providers may want to assign a peer of the auditor to review a draft internal audit report.[39]

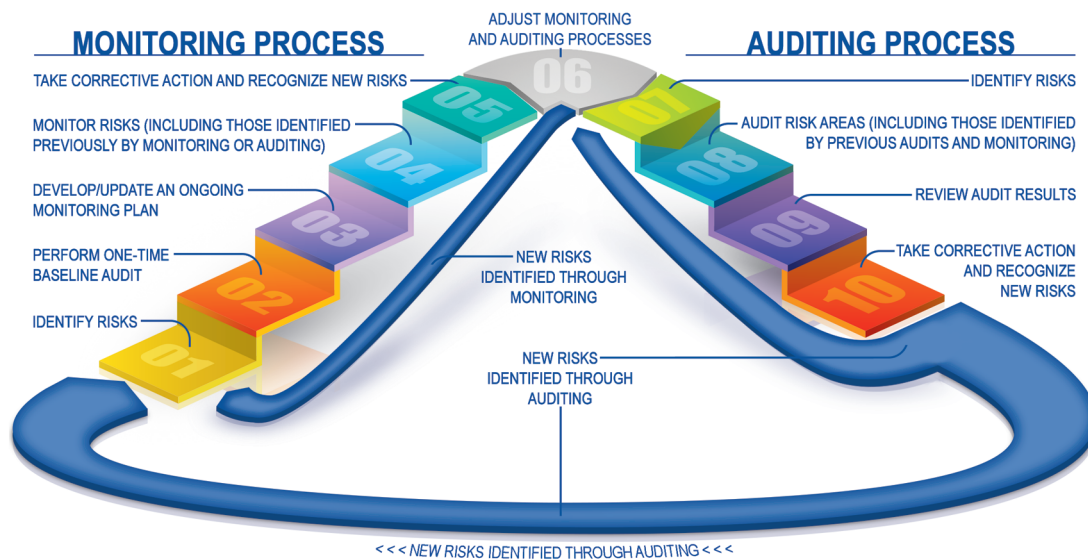
4. Review and Act on the Audit Results

Once an audit has taken place and been documented appropriately, the provider needs to follow up. For example, if the audit shows that an employee has violated policy regarding access to or dissemination of EHRs, the provider should promptly initiate appropriate disciplinary action. Report criminal violations to law enforcement in the manner required by the provider’s contract.

If the audit identifies EHR fraud, waste, or abuse that the monitoring program did not detect, modify the monitoring program to effectively detect fraud, waste, or abuse. Modification can take the form of changing the monitoring software or changing the monitoring policy. Depending on the nature of the violations identified, the provider may also want to institute or modify employee training.

Monitor and measure the efficacy of changes during the next regular audit cycle. As in any quality improvement activity, evaluate changes when implemented. If they are not effective, revise them. Following an audit, the monitoring response team should review the results to identify risk areas in the audit they should include in the ongoing monitoring plan. Figure 1 illustrates the dynamic relationship between monitoring and auditing.

Figure 1. Relationship Between Monitoring and Auditing



Conclusion

Providers can help detect and prevent fraud, waste, and abuse associated with EHRs by establishing processes for monitoring and auditing their EHR systems. Use review or audit to further analyze suspicious incidents detected during monitoring. In addition, providers should institute periodic internal audits of identified risk areas. Providers can use the audit results to correct violations, make appropriate referrals, and improve systems for preventing and detecting fraud, waste, and abuse in EHRs.

To see the electronic version of this job aid and the other products included in the “Electronic Health Records” Toolkit posted to the Medicaid Program Integrity Education page, visit <https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/edmic-landing.html> on the CMS website.

Follow us on Twitter  [#MedicaidIntegrity](https://twitter.com/MedicaidIntegrity)

References

- 1 Centers for Medicare & Medicaid Services. (2014, June 26). Affordable Care Act Provider Compliance Programs: Getting Started Webinar (Slide 26). Medicare Learning Network. Retrieved April 11, 2016, from <https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/MLN-Compliance-Webinar.pdf>
- 2 Kusserow, R.P. (2014, September-October). Claims Processing Ongoing Monitoring and Auditing: Improves Revenue and Prevents Costly Errors (pp. 45-46). Journal of Health Care Compliance. Retrieved April 11, 2016, from http://www.compliance.com/wp-content/files_mf/jhcc_091014_kusserow.pdf
- 3 Centers for Medicare & Medicaid Services. (2014, June 26). Affordable Care Act Provider Compliance Programs: Getting Started Webinar (Slide 28). Medicare Learning Network. Retrieved April 11, 2016, from <https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/MLN-Compliance-Webinar.pdf>
- 4 Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191, §§ 262, 264, 110 Stat. 196. Retrieved April 11, 2016, from <http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>
- 5 45 C.F.R. pts. 160, 164. Retrieved April 11, 2016, from <http://www.ecfr.gov/cgi-bin/text-idx?SID=1a6fd6d86be254e4c2011ad1d0045ba5&tpl=/ecfrbrowse/Title45/45CsubchapC.tpl>
- 6 45 C.F.R. §§ 164.302, 164.306, 164.530(c). Retrieved April 11, 2016, from http://www.ecfr.gov/cgi-bin/text-idx?SID=81320ec41eb3eb8ad72adfd2df6c2ff2&tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl
- 7 45 C.F.R. § 160.404(b)(2). Retrieved April 11, 2016, from http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=1001176da38a56b24f8899c788f9b5fa&n=sp45.1.160.d&r=SUBPART&ty=HTML#se45.1.160_1404
- 8 Specific Requirements, 42 C.F.R. § 438.608(b). Retrieved April 11, 2016, from http://www.ecfr.gov/cgi-bin/text-idx?SID=86e51d80c638deecda3e627fbc1d7270&mc=true&node=se42.4.438_1608&rgn=div8
- 9 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Physician Practices. 65 Fed. Reg. 59434, 59436. Retrieved April 12, 2016, from <http://oig.hhs.gov/authorities/docs/physician.pdf>
- 10 Foundation of Research and Education. American Health Information Management Association. (2005, September 30). Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities (p. 33). Retrieved April 14, 2016, from <http://library.ahima.org/PdfView?oid=65229>
- 11 Hom, D. (2014, September 30). Predictive Analytics—Detecting Fraud, Waste and Abuse in Health Insurance Exchanges. SCIO Health Analytics. Retrieved April 11, 2016, from <http://www.sciohealthanalytics.com/blog/exchanges/post/predictive-analytics-detecting-fraud-waste-and-abuse-health-insurance-exchanges>
- 12 U.S. Department of Health and Human Services. Office of Inspector General. (2014, January). CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs. Retrieved April 11, 2016, from <http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf>
- 13 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule. 45 C.F.R. 170 § 315(d). Retrieved April 11, 2016, from <https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf>
- 14 Centers for Medicare & Medicaid Services. Medicare Learning Network. (2014, June 26). Affordable Care Act Provider Compliance Programs: Getting Started Webinar (Slide 16). Retrieved April 11, 2016, from <https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/MLN-Compliance-Webinar.pdf>
- 15 Centers for Medicare & Medicaid Services. (2014, September 24). Managed Care Plans: Critical Partners in the Fight Against Fraud, Waste, and Abuse in Medicaid (p. 3). Retrieved April 11, 2016, from <https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Provider-Education-Toolkits/Downloads/managedcare-preshandout100114.pdf>
- 16 Centers for Medicare & Medicaid Services. (2013, January 11). Medicare Managed Care Manual. Chapter 21, Section 50.6.2. Retrieved April 11, 2016, from <https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/mc86c21.pdf>

- 17 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Physician Practices. 65 Fed. Reg. 59434, 59437. Retrieved April 11, 2016, from <http://oig.hhs.gov/authorities/docs/physician.pdf>
- 18 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule. 45 C.F.R. 170 § 315(d). Retrieved April 11, 2016, from <https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf>
- 19 American Health Information Management Association. (2014, March). Privacy and Security Audits of Electronic Health Information (2014 Update). Retrieved April 14, 2016, from <http://library.ahima.org/doc?oid=300276>
- 20 Minnesota Department of Health. (2013, February). Minnesota Health Records Access Study (p. 20). Retrieved April 11, 2016, from <http://www.health.state.mn.us/e-health/hras/hras021913report.pdf>
- 21 Boxwala, A., Kim, J., Grillo, J., & Ohno-Machado, L. (2011, May 2). Using Statistical and Machine Learning to Help Institutions Detect Suspicious Access to Electronic Health Records. *Journal of American Medical Informatics Association*, 18(4), 98, 500, 504. Retrieved April 11, 2016, from <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3128412/>
- 22 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. 65 Fed. Reg. 59434, 59437. Retrieved April 11, 2016, from <http://oig.hhs.gov/authorities/docs/physician.pdf>
- 23 Mosby's Medical Dictionary 8th ed. (2009). Definition of Incident Report. Retrieved April 12, 2016, from <http://medical-dictionary.thefreedictionary.com/incident+report>
- 24 Wisconsin Department of Health Services. (2015, August). Incident Reporting—Medicaid Waiver Programs—Instructions (pp. 2–3). Retrieved April 12, 2016, from <https://www.dhs.wisconsin.gov/forms1/f2/f22541i.pdf>
- 25 State of California. California Information Security Office. (2013, September). Incident Reporting and Response Instructions. Retrieved April 12, 2016, from http://www.cio.ca.gov/Government/IT_Policy/simm/simm5340_a.pdf
- 26 Skrocki, M. (2013, August 5). Can Plagiarism Detection Tools Catch EHR Upcoding? *Government HealthIT*. Retrieved April 12, 2016, from <http://www.govhealthit.com/news/how-plagiarism-detection-tools-could-catch-ehr-upcoding>
- 27 O'Reilly, K. (2013, February 4). EHRs: “Sloppy and Paste” Endures Despite Patient Safety Risk. *American Medical News*. Retrieved April 12, 2016, from <http://www.amednews.com/article/20130204/profession/130209993/2/>
- 28 McMillan M., Aske J., Terra M., & Fabbri D. (2013). Managing the Insider Threat: Real-Time Monitoring of Access Patterns to ePHI (p. 16). National Institute of Standards and Technology. Retrieved April 12, 2016, from http://csrc.nist.gov/news_events/hipaa-2013/presentations/day2/mcmillan_aske_fabbri_terra_day2_315_managing_the_insider_threat.pdf
- 29 McMillan M., Aske J., Terra M., & Fabbri D. (2013). Managing the Insider Threat: Real-Time Monitoring of Access Patterns to ePHI (p. 16). National Institute of Standards and Technology. Retrieved April 12, 2016, from http://csrc.nist.gov/news_events/hipaa-2013/presentations/day2/mcmillan_aske_fabbri_terra_day2_315_managing_the_insider_threat.pdf
- 30 Centers for Medicare & Medicaid Services. (2013, January 11). Medicare Managed Care Manual. Chapter 21, Section 50.6.2. Retrieved April 12, 2016, from <https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/mc86c21.pdf>
- 31 Centers for Medicare & Medicaid Services. (2014, June 26). Affordable Care Act Provider Compliance Programs: Getting Started Webinar (Slide 31). Medicare Learning Network. Retrieved April 12, 2016, from <https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/MLN-Compliance-Webinar.pdf>
- 32 Centers for Medicare & Medicaid Services. (2014, June 26). Affordable Care Act Provider Compliance Programs: Getting Started Webinar (Slide 29). Medicare Learning Network. Retrieved April 12, 2016, from <https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/MLN-Compliance-Webinar.pdf>

- 33 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. 65 Fed. Reg. 59434, 59437. Retrieved April 12, 2016, from <http://oig.hhs.gov/authorities/docs/physician.pdf>
- 34 Kusserow, R. P. (2014, September-October). Claims Processing Ongoing Monitoring and Auditing: Improves Revenue and Prevents Costly Errors (p. 46). Journal of Health Care Compliance. Retrieved April 12, 2016, from http://www.compliance.com/wp-content/files_mf/jhcc_091014_kusserow.pdf
- 35 Centers for Medicare & Medicaid Services. (2013, January 11). Medicare Managed Care Manual. Chapter 21, Section 50.6.5. Retrieved April 12, 2016, from <https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/mc86c21.pdf>
- 36 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. 65 Fed. Reg. 59434, 59437–38. Retrieved April 12, 2016, from <http://oig.hhs.gov/authorities/docs/physician.pdf>
- 37 Mazarredo, Y., & Munroe, F. (2012, March 9). Risk Assessments: From a Compliance Audit and Internal Audit Perspective (pp.13–19). Health Care Compliance Association. Retrieved April 12, 2016, from http://www.hcca-info.org/portals/0/pdfs/resources/conference_handouts/compliance_institute/2012/p7print2.pdf
- 38 U.S. Government Accountability Office. (2011, December). Government Auditing Standards. (Para. 6.03, p. 124). Retrieved April 12, 2016, from <http://www.gao.gov/assets/590/587281.pdf>
- 39 Bradshaw, R. (2000, April). Using Peer Review for Self-Audits of Medical Record Documentation. American Academy of Family Physicians. Retrieved April 12, 2016, from <http://www.aafp.org/fpm/2000/0400/p28.html>

Disclaimer

This job aid was current at the time it was published or uploaded onto the web. Medicaid and Medicare policies change frequently so links to the source documents have been provided within the document for your reference.

This job aid was prepared as a service to the public and is not intended to grant rights or impose obligations. This job aid may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. Use of this material is voluntary. Inclusion of a link does not constitute CMS endorsement of the material. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

June 2016

